L8: Entry 94 of 124 File: USPT May 15, 2001

DOCUMENT-IDENTIFIER: US 6233565 B1
TITLE: Methods and apparatus for internet based financial transactions with evidence of payment

Abstract Text (1):
A system and methods for conducting Internet based financial transactions between a client and a server. The client has a processor, a printer, a client authentication module, a module for issuing a transaction request, and a unique digital signature. The server has a network including a transaction server, a transaction database, a server authentication module, and a receipt generation module. An internet connection is used between the client and the server network. The transaction execution system includes authentication, wherein the client authentication module and the server authentication modules communicate via the internet connection and are authenticated to each other. A transaction module is included wherein, in response to the client and server being authenticated, the client issues a transaction request to the server and the transaction server, in response to a client transaction request, executes an electronic payment transaction at the server and records the transaction in the transaction database. The server receipt generation module, in response to an executed electronic payment, then generates a receipt and transmits the receipt to the client. The receipt includes the client digital signature and a data set uniquely identifying the executed transaction and is printable by the client printer. The printed receipt is an evidence of payment for the executed transaction. In addition, a third party seller having a processor and a database can be connected via a communication channel to the server, wherein the client further obtains a registration certificate representative of being a consumer registered with said third party seller. A third party credit facility also may be connected via a communication link to the server, for implementing credit card transactions. The transaction execution system may be to purchase an amount of postage, to purchase a ticket for air travel or to an entertainment complex or the like.

Brief Summary Text (2):
The present invention is directed towards electronic financial transactions between a customer having a personal computer (PC) and a remote service provider via the Internet, more particularly between a large plurality of customer PCs ("clients") and a remote service provider ("server"), wherein each transaction is digitally signed by the originator and is executed by the remote server, and a unique evidence of payment for the transaction is provided to the customer.

Brief Summary Text (4):
The inventors have recognized that there exists a Small Office/Home Office ("SOHO") business segment market which is driven largely by "immediate gratification" and cost sensitivity. That is, the entrepreneurs who comprise this market are more inclined to utilize a product or service if it can be accessed quickly with a minimum of red tape. There is a strong inclination for people in this market to place a very high premium on their own time and that of their employees, such that products that improve their efficiency are of great value.

Brief Summary Text (6):
A product or service that can be remotely accessed in real time would be highly

valued by SOHO (and non-SOHO) businesses whose livelihoods depend on access to electronic marketing methods worldwide.

Brief Summary Text (7):
The Metering Technology Management Office of the United States Postal Service ("USPS") has announced plans and issued regulations for a personal computer ("PC") based system for selling postage to individual customers under the Information Based Indicia Program ("IBIP"). See, for example, IBIP Host System Specification (Oct. 9, 1996), IBIP Postal Security Device Specification (Jun. 13, 1996), IBIP Indicium Specification (Jun. 13, 1996), IBIP Key Management Plan (Apr. 25, 1997), USPS Domestic Mail Manual, Issue 50 (Jul. 1, 1996), Federal Register, Part V, 39 CFR Parts 111 and 501 (Jun. 9, 1995), FIPS PUB 140-1 (January 1994), FIPS PUB 180-1 (Apr. 17, 1995), FIPS PUB 186 (May 19, 1994). The IBIP program products and services represent a significant paradigm shift from the traditional postage meter technology and processes in which the customer has custody of a device, the postage meter, and must take it or some part of it to the postal service office to purchase and refill the meter with more postage.

Brief Summary Text (8):
Protecting the security of the mails, United States postage funds, and the funds of the individual user and electronic commerce are of great importance. Improved apparatus and methods for providing such postal service transactions are desirable.

Brief Summary Text (9):
It is, therefore, an object of the present invention to provide customer (client) to remote service provider (server) electronic transactions which are secure and reliable.

Brief Summary Text (10):
It is another object to present a significant paradigm shift, building and improving upon current IBIP modeling, and to provide a software-only product utilizing the Internet, conventional and security (encryption) technology and a unique form of evidence of payment for executing secure electronic transactions.

Brief Summary Text (14):
Broadly, the invention concerns a system for electronic commerce including at least one user and a remote service provider, an Internet connection between each user and the remote service provider, wherein the user first becomes a registered user, e.g., registering with the remote service provider or with a third party supplier of goods and/or services or both, thereby obtaining a password set, and thereafter executes electronic transactions with the remote service provider using the password set to authenticate the user as a registered user and the remote service provider as an authentic service provider, and receives a secure evidence of payment for each transaction executed including a digital signature and data uniquely identifying the transaction.

Brief Summary Text (15):
In one embodiment, such a system may be implemented as follows. The system software is resident on a proprietary website of a remote service provider (hereinafter referred to synonymously as "RSP") and used to conduct commerce electronically with reliable security and confirmation, namely, evidence of payment. The RSP may sell services on its own account or act as a transaction intermediary between the customer and a third party seller ("TPS") that is offering the goods and/or services that the customer wishes to buy. The potential customer and user first registers and requests a license. The potential registrants are preferably licensed by the ultimate provider of the goods or services that will be purchased, for any of a number of reasons, including recordkeeping, billing, shipment, scheduling, warranty, etc., which may be the TPS or the RSP. In the case of the preferred embodiment, the user is licensed by the TPS which is the United States Postal

Service and which has established USPS specifications for licensing individual customers. Other "postal" services such as the Royal Mail of the UK, or a shipping company such as UPS or Federal Express and the like, also may have certain licensing procedures. Licensing or registration with the TPS may be as simple as obtaining a unique account number, or more complex as involving credit checks, references and collateralizations, as the case may be. In certain cases, a license from the TPS is not required and can be omitted, or a license may be available from the RSP for security reasons. The customer's license is then registered with the RSP and sent to the customer via regular mail.

Brief Summary Text (16):
The customer and potential user then uses the provided account information to download the appropriate portion of the system software (also referred to as the "client" software) from the RSP. The potential user then installs the client software on a local PC type device and configures the software and hardware of the system for use including establishing a transaction database specific to the user. This database may include a Register indicating purchases or funds available or the like. The system also provides for authenticating the user to the RSP and the RSP to the user before any transaction can occur.

Brief Summary Text (17):
After authentication is completed, the user then purchases the ultimate goods or services, postage in the case of the preferred embodiment, utilizing credit cards, ACH debit cards or checks as the method of payment, and electronically confirming the sale. The RSP then operates on the user's transaction database, e.g., increments a "descending" register, associated with the specific user corresponding to postage purchased by the user. The transactional database for the user is maintained by the RSP and uses special transactional software, which for postage is referred to as a Postal Security Device (PSD) software, resides on a server of the RSP, and manages the accounting, auditing, and security, digitally signing each transaction to identify uniquely both the user and the transaction. The special transaction software also manages the printing at the user of evidence of payment of the purchase, e.g., postage, postage corrections, and refunds, and other miscellaneous communications with the RSP as appropriate and the TPS of goods or services, in the case of the preferred embodiment the United States Postal Service. Should there be a problem with the authentication process, the RSP server would disable the descending register and report the failure to the appropriate USPS authority, e.g., the National Meter Accounting and Tracking System ("NMATS"). Should there be a problem with the user's registration/license or should fraud be detected, e.g., detecting the same evidence of payment more than one time, the RSP server would disable the descending register and report the failure to NMATS. Should the user wish to terminate use of the product, the client software locally downloaded can be automatically uninstalled, disabling and rendering inoperable all aspects of the system software for the user. Uninstalling the client software would result in revocation of the customer's license. This revocation will be reported to the appropriate authority, e.g., the Centralized Metering Licensing System ("CMLS"). Any subsequent use of the "retired" password or account numbers by that or any other user constitutes fraud, which is detectable.

Brief Summary Text (18):
In an alternative embodiment, the transaction also may be digitally signed by the RSP executing the transaction, as well as by a TPS who provides the goods or services, thereby uniquely identifying the transaction in more detail.

Brief Summary Text (19):
Another aspect of the present invention is directed to a postal purchase system. One such system includes, for each customer, a client system and a Postal Secure Device (PSD) as defined by the IBIP specifications. The client system is a Host which resides on the customer's local PC and is responsible for the following: mailing list management, capturing postal purchase and refund request information,

and providing an interface to the local printer producing the postal indicia. Each customer's PSD resides at a RSP "server" site and can be accessed only via the Internet. The customer's PSD is responsible for managing ascending and descending registers which track postal transactions, and creating a digital signature for each postal indicium produced by the customer on the local printer. By keeping all PSD functionality on a remote, central station server/network, all cash and key management and process auditing can be centralized and secured.

Brief Summary Text (20):
One embodiment of a system for conducting Internet based financial transactions including:

Brief Summary Text (21):
a client having a processor, a printer, a client authentication module, a module for issuing a transaction request, and a unique digital signature;

Brief Summary Text (22):
a server having a network including a transaction server, a transaction database, a server authentication module, and a receipt generation module; and

Brief Summary Text (24):
wherein the transaction execution system further comprises:

Brief Summary Text (26):
a transaction module wherein, in response to the client and server being authenticated, the client issues a transaction request to the server and the transaction server, in response to a client transaction request, executes an electronic payment transaction at the server and records the transaction in the transaction database, and wherein the server receipt generation module, in response to an executed electronic payment, generates a receipt and transmits said receipt to the client, said receipt comprising the client digital signature and a data set uniquely identifying the executed transaction; and

Brief Summary Text (27):
wherein the receipt is printable by the client printer and the printed receipt is an evidence of payment for the executed transaction.

Brief Summary Text (28):
In one embodiment, the module for issuing a transaction request further comprises a means for providing the transaction request with the client digital signature, and the server further comprises a unique digital signature and the receipt further comprises the server digital signature.

Brief Summary Text (29):
The server may include a first server, a firewall and a single TCP/IP port, such that the first server is connected to the internet connection, the firewall is interposed between the first server and the transaction server and the transaction server is connected to the network through the single TCP/IP port. In this embodiment, the firewall comprises a communication module that operates to limit communications between the internet and the transaction server to client transaction requests identifying the single TCP/IP port.

Brief Summary Text (30):
Preferably, the system also includes a third party seller having a processor and a database, and a communication channel between the third party seller and the server, wherein the client further comprises a registration certificate representative of being a consumer registered with said third party seller. In such a system, a transaction module is provided and the third party seller database is updated by said server transaction database.

Brief Summary Text (31):
In an alternate embodiment, the system optionally may include a third party credit facility and a communication link between the third party credit facility and the server, wherein the server has a credit module and, in response to a suitable client transaction request, a credit card payment request is made by the server to the third party credit facility, the third party credit facility authorizes the credit card payment and issues an authorization code to the server, and the server transaction database is appropriately updated.

Brief Summary Text (32):
In an alternate embodiment of the system, the transaction request may include a request to purchase an amount of postage, an addressee data set, and wherein the server transaction database further comprises a pool of postage prepaid by said server, and an account register associated with said client, wherein the client transaction request operates to transfer the requested amount of postage from said pool to said client account register.

Brief Summary Text (34):
Another aspect of the invention is directed to a method for conducting Internet based financial transactions. One such method includes:

Brief Summary Text (35):
(a) providing a client having a processor, a printer, a client authentication module, a module for issuing a transaction request, and a unique digital signature;

Brief Summary Text (36):
(b) providing a server having a network including a transaction server, a transaction database, a server authentication module, and a receipt generation module;

Brief Summary Text (39):
(e) issuing a transaction request from the client to the server;

Brief Summary Text (40):
(f) in response to a client transaction request, executing an electronic payment transaction at the transaction server and recording the transaction in the transaction database, generating a receipt at the server receipt generation module, providing said receipt with the client digital signature and a data set uniquely identifying the executed transaction, and transmitting said receipt to the client; and

Brief Summary Text (41):
(g) printing said receipt using the client printer, wherein the printed receipt is an evidence of payment for the executed transaction.

Brief Summary Text (42):
In one embodiment, step (e) includes providing the transaction request with the client digital signature, step (b) includes providing the server with a unique digital signature, and step (f) includes providing the server digital signature as a part of the receipt.

Brief Summary Text (43):
In a preferred embodiment, step (b) includes providing a single TCP/IP port connecting the first server to the internet connection with the client and limiting communications between the internet and the transaction server to client transaction requests identifying the single TCP/IP port.

Drawing Description Text (3):
FIG. 1 is a block diagram of an architecture of an Internet-based transaction

system in accordance with a preferred embodiment of the present invention;

Drawing Description Text (4):
FIG. 1A is a diagram of the transaction and maintenance functions of the system of FIG. 1;

Detailed Description Text (3):
FIG. 1 also shows the relationship between a plurality of individual PSDs 20n, where n=i, j and k corresponding to three different hosts 10i, 10j, and 10k and customers 2i, 2j, 2k respectively, and a single master PSD 40. The master PSD 40 is responsible for all cash management functions with the TPS server/network 6. In the preferred embodiment, the TPS 6 is the IBIP infrastructure as defined by the U.S. Postal Service IBIP specifications, and the master PSD 40 maintains a "pool" of postage with which the individual PSDs 20n transact business.

Detailed Description Text (4):
Customer 2n transactions occur between the customer's PSD 20n and the master PSD 40 over a secure bus 50, at RSP 4. Postage purchase transactions and funds flow occur between the master PSD 40 and the Computerized Meter Resetting System ("CMRS") infrastructure 60 of the United States Postal Service Treasury (the "Treasury") as referenced in the published CMRS specifications, IBIP Postal Security Device Specification Jun. 13, 1996, referred to herein as IBIP Finance infrastructure or TPS 6, by a private network connection 8. Each customer 2n also has a local printer 70n associated with each Host 10n for printing the postage indicium and reports as will be described.

Detailed Description Text (5):
The infrastructure of the RSP (or "server") 4 is preferably designed to address the following goals: (1) It will meet all Level 2 security requirements as defined in the aforementioned FIPS 140-1 and FIPS 186 specification, except for physical security because the transaction server(s) 180 on which the PSDs 20n and Master PSD 40 reside will exist on a protected segment behind a firewall 160 (see FIG. 2). Security measures are used to ensure that the transaction server 180 is physically accessed by highly trusted and authorized individuals only; (2) It will be scalable from zero to two million customers (n, n=1 to 2.times.10.sup.6 customers); (3) Customer Host 10n requirements are a personal computer ("PC") with a 486 processor or higher, 8 Megabytes of RAM, a hard drive with at least 10 Megabytes of space available, a modem (9600 BPS or higher), a printer (laser, inkjet, or bubblejet), running preferably Windows95.TM., a web browser software, and an active Internet connection; (4) Non-print electronic transactions should be performed in less than five seconds; and (5) Print electronic transactions should be completed within thirty seconds.

Detailed Description Text (6):
Referring to FIG. 2, the infrastructure of RSP 4 can be broken down into several pieces: (1) A web server 150 that is used by customers for registration and client software download and is the apparent website; (2) A transaction server(s) 150 that serves as the transactional link between the customer's Host PC 10n and all RSP 4 functions; and (3) A series of database servers 170 that perform all of the RSP 4-related and TPS 6-required functions.

Detailed Description Text (7):
Referring also to FIG. 2, to protect the various components from unauthorized access and intrusion, the PSP 4 is provided with an inbound network 110 and an outbound network 130. The inbound network 110 allows a customer 2n to securely access the RSP web server 150. The outbound network 130 allows for the secure exchange of financial transactions executed between the customer 2n and the TPS 6 directly and/or indirectly through RSP 4. Network traffic in and out of these networks is controlled by a conventional inbound router 112 and an outbound router 132, which will operate to filter out all unauthorized traffic. In addition, a

firewall 160 will be used on the inbound and outbound segments to examine each data packet transmitted for proper authorization. The secured portion of the RSP web server 150, i.e, that portion which is access protected by passwords to authorized/registered users, will exist on a unique port 140 so that only traffic identifying that specific port 140 will be accepted. The transaction server(s) 180 will exist on a unique internet protocol ("IP") address(es) so that the outbound router 132 can filter out all traffic except to that address. The transaction server 180 will also be configured to handle IP traffic only. The outbound router 132 and the firewall 160 will filter out all other Internet protocols according to industry standards for such firewalls. The PSP 4 also includes a series of data servers 170 (shown collectively in FIG. 2) that will be responsible for various dedicated functions. As the transaction server 180 receives a transaction request, the type of transaction is identified and processed using one of these servers as identified in the Table I below.

Detailed Description Text (8):
Scalability is maintained by allowing for multiple servers, particularly for the transaction 180, payment 190, and log 195 servers (multiple servers not shown). These servers will process the highest volumes of traffic because all transactions will pass through them.

Detailed Description Text (9):
Preferably, various other software manufacturers will be able to develop and/or access both the printing and transaction management pieces of the system through a controlled set of Application Program Interfaces (API) for each customer 2n to operate the system using a conventional word processing or x-window motif program and the downloaded client software.

Detailed Description Text (17):
At step 212, after receiving the letter, the customer uses its Internet browser again to connect to the RSP web server 150. The customer selects a SOFTWARE DOWNLOAD option at step 213, and is prompted for the customer number and password to enter the secured area of web server 150 at step 214. Once the customer password and identification is entered and verified, at step 215 the web server 150 retrieves the previously stored customer record. At step 216, the customer then downloads the client software program for operating the system, the internet protocol address for postal transactions, the public key/private key pair for the RPS 4, and the public key for TPS 6.

Detailed Description Text (22):
With reference again to FIG. 3 and to FIG. 6, after receiving the certificate and a license/registration number at step 216, the user 2n can then proceed to make a purchase, e.g., of postage. User 2n makes a purchase through a proprietary connection over the Internet 30 using the appropriate IP address as provided by the downloaded client software to connect with the RSP's Internet transaction server 180, utilizing a suitable form of payment, such as credit cards, electronic funds transfer, ACH debit cards, or checks.

Detailed Description Text (23):
Electronic payments are reported to the transaction server 180 which then transmits them to a specified financial institution for deposit. Upon receipt back of an authorization code, transaction server 180 then increments the user's descending register 21 in PSC 20n with the correct amount. The ascending and descending registers of each user 2n are stored on the Master Server 300 at RSP 4. Under current Postal Service guidelines, the total maximum amount permitted in the descending register 21 is $500.00, but any value could be used, as well as no limit at all.

Detailed Description Text (24):
Checks used to pay for postage are preferably sent by the user 2n to a designated

lockbox institution for processing in a conventional manner. When a user's check has cleared, the lockbox institution transmits an electronic authorization to the transaction server 180, which operates to transmit a notice to the user 2n of postage availability. The user 2n typically must then access the transaction server 180 to obtain the postage (which may have already been allocated to the user 2n and held in a suspense server 310) and server 180 operates the master server 300 to increment the user's descending register 21n in PSD 20n by the proper amount and clear the register in suspense server 310.

Detailed Description Text (31):
A portion of the system software resident on the transaction server 180 of RPS 4 functions as the Postal Secure Device (PSD) 20n. This software portion, known as the Transaction Manager, encompasses many features and benefits to both the TPS 6 (e.g., United States Postal Service) and customers, as illustrated by Table II.

Detailed Description Text (32):
The system of the present invention can be considered as a combination of several components or modules which include: UI (user interface), Security, Printing, Financial Transactions, Communications, and Database Management. Each of these is designed to be in compliance with industry standards, discussed below.

Detailed Description Text (39):
Financial Transactions

Detailed Description Text (40):
All purchase and refund requests will be digitally signed and encrypted for transmission from the host IOn to the transaction server 180. RC2 symmetric encryption standard key pairs (public key/private key) may be used to support such encryption and decryption. RC2 will be used to protect the nature of the purchase/refund request, which may include credit card information. RC2 is a well-known industry standard. RC2 is a product of RSA. RSA is an accepted vendor for these products according to the IBIP Indicium specification dated Jun. 13, 1996.

Detailed Description Text (41):
For credit card purchases/refunds the transaction from the transaction server 180 to the credit bureau 9 preferably will employ SSL3.0 (Secure Socket Layer) standard encryption for secure packaging of the transaction. SSL3.0 is an accepted industry standard for financial transactions across a TCP/IP network. Other suitable encryption standards could be used.

Detailed Description Text (45):
Database

Detailed Description Text (46):
The PSP 4 server 180 will store all transaction, customer, and PSD information in one or more industry standard databases, each preferably being an SQL database, using an SQL Server. This product has been adopted as an industry leader in relational database technology, although other relational database technologies could be used, as well as non-relational database technologies.

Detailed Description Text (48):
The software design preferably employs industry standards for both the object and database modeling. The Booch methodology may be employed to produce an industry standard object model. The James Martin methodology may be used to generate the data model. Rational Rose v4.0 can be used to capture the data for this methodology and for its output. ERWIN Data Modeler can be used to capture the data and generate the data model used by this product.

Detailed Description Text (56):
The customer 2n enters the download area of the web site 100 and is prompted to

enter the assigned customer number and customer password. These entries are checked against the customer record in the Master Database 305. If the customer number and password are valid, the download will proceed. In addition to the client software, the customer 2n will receive a public key and a private key pair file in encrypted form from the web server 150. The keys will be stored on the Host 10 in an encrypted form. The private key is decrypted by the customer password. This private key is then used by the customer 2n and the client software for creating a customer digital signature and for decryption. Since the web server 150 has the corresponding public key, (the server 150 generates the key pair provided to the registered user 2n) the server 150 can use the customer's public key to verify the user's digital signature and to encrypt the indicia 74 (or other data) for downloading to the customer 2n.

Detailed Description Text (60):
A function allows the user 2n to purchase postage from the PSP 4 transaction server 180. It is initiated by selecting a "Purchase Postage" screen in the client software. The screen displays the maximum postage that can be purchased, any fees associated with this purchase, which are charged by PSP 4 or TPS 6 as the case may be, and the total cost for the purchase. The customer 2n must enter an amount of postage to purchase and select a method of payment. The methods of payment are preferably shown with "radio" buttons and include credit card, ACH debit, and check. The default payment is preferably by credit card and the credit card input area is activated.

Detailed Description Text (61):
The customer then initiates transmission of all of the purchase information (e.g., addresses, purchase amount, and credit/check information) via the Internet 30 to the web server 150, which passes on the transaction request to the transaction server 180. When the Submit radio button is pressed, all customer information is digitally signed and encrypted and packaged with the purchase amount. A connection over Internet 30 is established with the web server 150 and the transaction related information is then transmitted. Because the transmission has the appropriate IP address for the transaction server 180 it will be directed by web server 150 through the firewall 160 to transaction server 180, where the transaction will be executed. If a connection cannot be made with the web server 150, then control is passed to an Unable To Connect Error. When the web server 150 responds, the text message received from the server 180 is displayed in the main message area at the top of the screen of the user's Host 10n. Possible responses include Purchase Complete, Incorrect Credit Card Information, Purchase Pending, or Credit Denied. If a Purchase Complete or Pending message is received, the descending register 21 (Postage Remaining field) specifically associated with the customer 2n in the PSD 20n is updated with the new value from the transaction server 180. The actual PSD registers 20n remain on the master server 300; the Host 10 merely displays a copy of the PSD 20n register 21 values.

Detailed Description Text (65):
After the user fills out the entire field on the purchase screen and selects a submit radio button, the transaction server 180 immediately constructs a new purchase request object base from these field values.

Detailed Description Text (66):
After the transaction server 180 receives the purchase request, it interacts with the following servers to execute the transaction:

Detailed Description Text (68):
2. Purchase server 190 (after the purchase request object is deciphered by the transaction server 180, it passes to the purchase server)

Detailed Description Text (69):
Credit card requests are transmitted to the web server 150 by the client, forwarded

to the transaction server 180, and then to a payment server 190, a credit authorization server 400, and to a remote credit bureau 9 such as to First Data Merchant Services ("FDMS"). The credit authorization server 400 is responsible for connecting to the credit card bureau 9 and getting approval: A "result" code is passed back to the purchase server 190 to indicate whether the credit card has been approved or not. For example, 0 means on the credit link is down (after 3 attempts), 1 means the credit card was rejected, and 2 means the purchase is approved.

Detailed Description Text (71):
If payment is by check, the check number is sent to the web server 150 and purchase server 190 along with the information listed above. The response from the purchase server 190 will include a customer number. When the response is received at the Host 10n from the transaction server 180 then control is passed to the Remittance Pop-Up Window.

Detailed Description Text (72):
Check purchasing is very similar to credit card purchasing. The difference is that the purchase server 190 does not need to go through the credit authorization server 400 to obtain any credit approval and typically has a suspense server 310 to enable check processing prior to issuance of postage. Because the check purchasing cannot be validated right away, the purchasing server 190 invokes the Persistence Service and Database Service to update the database record, logging the transaction and updating the descending register in the PSD object. See Logging 196; Customer PSD 200 (increment); Master PSD 40 (decrement) in FIG. 3.

Detailed Description Text (77):
The customer then must enter in credit card, debit card, or check information so that the appropriate account can be credited or a check can be issued. The user presses the Submit button to submit the request to the web server 150 and then to the transaction server 180. For a spoilage refund, a copy of the updated descending register 22 is received from the server 180. The actual descending register 22 is updated on the server 20n.

Detailed Description Text (79):
i. Transaction Complete

Detailed Description Text (80):
In each of the foregoing transactions, once a transaction is completed, transaction server 180 creates a response transaction which is digitally signed with the digital signature of the customer 2n requesting the transaction, encrypted, and sent to the Host 10n confirming the success or failure of the transaction. The host then updates its local information to reflect changes in postage available.

Detailed Description Text (82):
A configuration feature is desired to allow the user to change the configurable settings for the Host 10n system. It is initiated by selecting a Configure screen including radio buttons for selecting the method of logging postage usage and the address cleansing method. The screen also may contain two postage threshold entry fields and a drop-down list box for selecting a printer 70n. The user 2n is required to make selections for certain settings in a conventional manner. Optionally, log postage can be selected, which the user can use for accounting purposes. Postage usage will differ from the indicium, which is always logged on the Log Server 195. The Log database 196 DB is used to track all transactions between customers and RSP 4. The central database 197 is a staging server used to create data files for transmission to TPS 6, e.g., USPS. The indicium 74 represents a unique identifier that is digitally signed for each mail piece. Logging postage usage would store a log of the address of each letter or label, the date printed, and the amount of postage for that mail piece in a log database 196. This information may or may not be unique because multiple letters could be sent to the

same address on the same day. The indicium 74, however, will always be unique and digitally signed. Logging postage usage is the default.

Detailed Description Text (91):
With respect to maintaining logs databases 196, 197 of indicia files on the transaction server 180, it is expected that the United States Postal Service will permit these files to periodically be off loaded onto tape, or otherwise transmitted periodically. See, e.g., FIG. 1A, the reference to "batch" connecting data management functions 42 and 62.

Detailed Description Text (94):
Preferably, the system permits the user to preview a single envelope or label by pressing a Print Preview button. This will cause the return address, the mailing address, and a bitmap of a sample indicium 74 to be displayed as it would appear printed. Pressing this button will pass control to a standard Print Preview screen. If the user wishes to print the entire list, the Print All button is selected. Pressing Print All causes a connection to be made to the web server 150 and a file of addresses sent. This file is digitally signed by the client Host 10n for the transaction server 180 to verify. On the transaction server 180, the digital signature on the file will be verified by validation (also called the security) server 315, each address will be extracted individually and the contents of that address, along with additional information, will be used to create both the human- and computer-readable parts of the indicium 74. See indicium generation 43, FIG. 1A. The postage rate table used is checked to see if it is current, and the postage amounts are recalculated if needed. The contents of the indicium are then hashed (MD5) into a message format and the resulting message is digitally signed by transaction server 180 using the well-known DSA. The indicium is then encrypted for the client to decrypt. The indicium is encrypted to prevent unauthorized capture of the indicium. An unencrypted indicium could be captured, printed, and entered into the mail stream prior to it being obtained by the authorized customer.

Detailed Description Text (101):
A postage correction feature allows the user to print a correction indicium in the event that the postage amount or the postage date is incorrect. It is initiated by selecting a Correct Postage screen and choosing the appropriate correction for a postage amount or a postage date. Invalid information will be identified once valid information is provided. A connection is made to the PSP 4 server 150 and the correction transaction is validated. Notification is sent to the Host system 10n and the user is informed whether to place the envelope back in the printer 70 in the same direction as the first printing or to reverse it before printing.

Detailed Description Text (103):
The present invention advantageously uses the internet 30 connection for registration, client/server authentication, transmission of credit card information, transport of indicia, requests for refunds, change of personal/address information, and the exchange of addresses for cleansing. Each of these transactions will require different types of security to ensure the safe exchange of information between the Host 10n, PSD 20n, and printer 70n. Conducting financial transactions over an unsecured channel such as the internet 30 requires the use of cryptographic modules. In the present invention, each client 2n has a cryptographic module 12n and the RSP server 4 has a cryptographic module 14. The server cryptographic module 14 serves three functions: (1) authentication, (2) encryption, and (3) authorization. Authentication is the only function that requires interaction with a client cryptographic module 12. This is discussed below.

Detailed Description Text (104):
The physical architecture of the system of the present invention was designed to ensure that all access to the system is through secured and monitored points. The entire system that is at PSP 4 will reside on a private network and the transactional portions will be connected through a firewall 160 to the internet 30.

Firewall 160 will be configured to restrict all network traffic to a single TCP/IP port 140. All packets received by the firewall 160 on the specified port will be routed to a Transaction Manager (i.e., transaction server 180. It is noted that the actual implementation may have a plurality of transaction servers 180n, and routing a given packet to a transaction server 180 may be based on an address field in the packet or on a first available server, as the case may be. Once a transaction server 180n receives the packets that request a socket connection, a socket connection will be established. The transaction server 180 will immediately require that each particular connection authenticates a client 2n, or the connection will be dropped. To ensure this safe exchange, the implementation of security uses the following assumptions:

Detailed Description Text (105):
The host 10n and PSD 20n functions will not reside on the same machine. The PSD 20n functions will not be stored in a separate hardware device connected to the customer's PC. The Host 10n will exist on the customer's PC and the PSD 20n will exist on the PSP 4 network infrastructure. The Internet 30 will be used to interconnect a customer's host 10n and printer 70n with the PSD 20n. All transactions between the Host 10n and the PSD 20n will be encrypted. All transactions between the host 10n and the PSD 20n will be digitally signed. All indicia 74 will be digitally signed. All indicia 74 will be encrypted for client 10n to decrypt prior to printing. Prior to initiating a transaction, both the client 10n and the provider transaction server 180 will authenticate each other. A customer's actual existence and proof of valid physical address will be initially established by sending the system license and registration information to the customer by mail. All cash management functions will be performed within the treasury component of the RSP 4, namely, payment server 190, separate from the PSD 20n functionality.

Detailed Description Text (106):
The following discussion describes a preferred security model to be implemented. The downloaded client software performs all Host 10n and printer 70n functions, as defined by the appropriate IBIP specifications. The transaction server 180 performs all of the PSD 20n and TPS 6 infrastructure and support functions, as outlined by the IBIP specifications. Each client 2 and server 4 is comprised of its own cryptographic module 12 and 14, respectively. For authentication and key expiration/regeneration the two modules 12 and 14interact.

Detailed Description Text (131):
With reference to FIG. 8, the finite state model defines a preferred set of system access rules. The model defines secured and unsecured states and all state transitions. When the client software is executed, the client cryptographic module 12 initially enters a Self-Test State 910. The Self-Test State 910 is when all self-tests are performed. If all self-tests pass successfully the module proceeds to enter the Un-Initialized State 920, otherwise the module will enter into the Error State 950. When a client 2 to server 4 transaction is initiated, the cryptographic module 12 enters the User State 930 and/or the Crypto-Officer State 940 as described below.

Detailed Description Text (141):
The client 2 has no direct control over the services performed by the server cryptographic module 14. All services performed by the server cryptographic module 14 are under the direct control of a Transaction "Manager" server 180. Once the client 2 has been authenticated, it submits a transaction request to the transaction server 180 and waits for a response. It now becomes the job of the Transaction Manager to process the transaction and return a "receipt" to the client 2. All transaction "receipts" will contain a date/time stamp, and a sequence number and a digital signature to verify the authenticity of a transaction in relation to other similar transactions. For a given customer 2n, the sequence number will increase by one each time until a threshold is met, e.g., 10,000, at which point

the counter will reset to 1.

Detailed Description Text (142):
The Transaction Manager embodies the logic required to complete a transaction while enforcing the security and integrity of the server cryptographic module 14. Based on the authenticated user 2n, the transaction requested, the date/time stamp, and the sequence number, the Transaction Manger would determine whether the requested transaction is valid. The Transaction Manager will complete the transaction by sending a receipt, including a digital signature as evidence of payment for the transaction, back to the client 2n. In the case of the postage purchase system, the receipt is the indicium 74, which includes the foregoing and the postage related information (addresse, postage amount, etc.).

Detailed Description Text (143):
The Transaction Manager server 180 also is responsible for performing non-cryptographic functions. For example, address cleansing, credit approval and customer profile changes, which are performed by transaction server 180, do not require the use of cryptographic functions, and are therefor considered outside the realm of the server cryptographic module 14.

Detailed Description Text (148):
The server cryptographic module 14 manages cryptographic keys, certificates and PSD registers 21, 22. All sensitive data is stored in a Secure SQL Server Database and protected by SQL Integrated NT security. See FIG. 3. The Secure SQL Server database 305 is considered a part of the server cryptographic 14 module and may only be accessed by the cryptographic module.

Detailed Description Text (175):
The authentication service is responsible for ensuring that only authorized users 2n have the ability to submit transaction requests. It will utilize the client's public authentication keys to perform the user validation. Upon successful authentication the transaction manager (server 180) will handle the user's transaction request.

Detailed Description Text (181):
The Registration Service is outside of the cryptographic module 14. It is essentially responsible for adding new users to the PSP 4 system. It communicates with the Transaction Manager server 180 to generate a new encrypted user key file, which is later downloaded by the client 2.

Detailed Description Text (191):
The session keys generated during the authentication process are preferably 64-bit RC2 symmetric keys, which are used to encrypt and decrypt all data sent between the client and the server. A hash of the data value is appended to all transaction request data or a transaction receipt before it is encrypted and sent to the other party. The recipient uses the hash to ensure message integrity. If the message is found to be corrupt or altered in some way, the transaction will be aborted.

Detailed Description Text (194):
The transaction server 180 is concerned with two types of public/private key pairs, authentication and indicium generation. Authentication keys are 512-bit RSA keys and the indium generating keys will 1024-bit DSA keys. Both the client 2 and the server 4 each have a pair of authentication and indicium generating keys.

Detailed Description Text (197):
The client authentication keys will have an expiration period. The duration of this period will be, for example three (3) years, as determined by the USPS Key Management Specification. To prevent checking for key renewal every time a client 2n connects to the server 4, all client keys may be set to expire at the same time. After a client 2n authenticates with the server 4, the server 4 will notify the

client if its keys have expired. At that time, the client will generate a new set of keys and send the public key to the server. The server only stores the client's previous public authentication key. The private key is kept private with only the client. The public key is kept inside a password protected SQL master database 305 (FIGS. 4, 7) that is accessible only by the server cryptographic module 14. In the scenario when a user 2n requests a full refund, that user's keys are destroyed and their record removed from the SQL database 305.

Detailed Description Text (199):
The software product will execute a key generation routine. This routine will produce the server's public/private RSA 1024-bit authentication keys. The key will be stored on a secured SQL master database 305. The public/private keys will have an expiration period defined by the USPS. When the server's keys expire, it will regenerate a new pair of authentication keys. With every client record, a field will be used to indicate which version of the server public key its using. During authentication, the server 4 will retrieve the appropriate version of its authentication public key. If the client 2n is using an expired key, the server 4 will download the new key to the client 2n. The client's record will be modified to reflect the new key version. The server 4 will keep its old authentication keys archived for a specified period of time. This allows a client 2n who has not connected since the server's public key expired the ability to authenticate and download the server's current public key.

Detailed Description Text (203):
The client 2 and server 4 indicium keys are used to generate indicium 74 and all reside on the server 4. A client indicium key pair exists for every registered customer 2n while there is only one pair which exists for the server 4. All indicium key pairs are generated on the server 4. The private keys are immediately stored in the SQL master database 305, while the public keys are sent in a request to the Certification Authority of the USPS for certificate generation. The USPS will generate the certificates and send them to the server 4, which will verify the certificate's source and store it in a SQL master database 305.

Detailed Description Text (205):
The server 4 needs a public/private key pair for each client 2n in order to produce indicia. The server 4 will generate a key pair for the client 2n, store the private key in the secured SQL master database 305 and send the public key to the CA as a request. The request is signed with the server's private indicium key and sent to the CA, where the request will be authenticated using the server's certificate. The CA will send the certificate back to the server. The returned certificate will be packaged with some other information and digitally signed by the CA. Using the CA certificate the server 4 will verify the authenticity of this returned package.

Detailed Description Text (208):
The server cryptographic module 14 is responsible for completing the task of indicium generation. When an indicium generation request is passed to the cryptographic module 14 through one of its interfaces, the data included will be missing the client's indicium certificate and the PSD 20n register values. The cryptographic module 14 will retrieve the appropriate values from the SQL master database 305 and fill in the remaining values. The result is then signed with the client's private indicium key. The actual indicium 74 is the concatenation of data and the digital signature. Because of the presence of the client's certificate (which was signed by the USPS CA) the indicium 74 can be easily verified for authenticity by using the public key embedded in the client's 2 indicium certificate. The completed indicium 74 is returned back through the cryptographic module interface and ready to be sent to the client 2n. The data included in the indicium 74 can include, for example, the user 2n, the addressee of the recipient, the postage, the rate table used to calculate the postage, the date, time and preferred postal office/box/pickup location, etc.

Detailed Description Text (210):
The PSDs 20n will actually reside on the secured SQL master database 305, although illustrated separately on FIG. 3. Each client 2n will have its own record representing its PSD 20n, while the server will have one master PSD 40.

Detailed Description Text (212):
The Master PSD 40, also resident on master database 315, contains three fields: Ascending Register 44, Descending Register 45, and Refund Register 46. The Ascending Register 44 measures the total dollar amount of postage that the server has sold to clients. The Descending Register 45 measures the total dollar amount of postage that the Server has to sell to clients. The Refund Register 46 measures the total dollar amounts of postage that server have refunded to clients.

Detailed Description Text (224):
StoreClientPublicKey (PublicKey [in], status [in]) This interface will allow the client's public authentication key to be updated in the cryptographic module's database. The status will indicate whether the function completed successfully.

Detailed Description Text (227):
Referring to FIG. 8 again, the finite state model defines the set of system access rules for the server cryptographic module 14. The model defines secured and unsecured states and all state transitions. When the software is executed, the cryptographic module 14 enters the Self-Test State 910. For example, the first test will verify that the executable module check-sums are correct. This will ensure that none of the code has been corrupted or modified. Next, the cryptographic algorithms will be tested. The RSA, RC2 and MD5 cryptographic algorithms will be tested using the "known-answer" test. A known value will be applied to the algorithm to determine if it will reproduce a known result. If the resulting value matches the expected result, the algorithm is assumed to be functioning properly. Since the DSA algorithm does not reproduce the same value twice, it will use pair-wise consistency test. This test will first sign a quantity with a private key and then verify the signature of this quantity using the public key. If the result of the verification is successful, the test succeeds. If any of cryptographic modules tests fail, it is assumed to be malfunctioning. If all self-tests pass successfully, the module proceeds to enter the Un-Initialized State 920, otherwise the module will enter into the Error State 950. No keys are loaded into the module during the Un-Initialized State and therefore no cryptographic functions can be performed. It is in this state that authentication service starts. Based on the authenticated user and the requested transaction, the cryptographic module will determine whether the next state should be the Key Entry State 960 or the Crypto-officer State 940. This decision will depend on whether the transaction will use the cryptographic module to perform key management or other cryptographic functions.

Detailed Description Text (228):
Because the transactions of multiple clients 2n will be handled simultaneously, the cryptographic module 14 will support a finite state machine that can be in the Idle State 970, Key Entry State 960, and Crypto-Officer State 940 at the same time. If key management functions are called, the module 14 enters the Crypto-officer State 940. In the Idle State 970, all cryptographic keys have been loaded into the module. The module is now initialized and remains idle until cryptographic functions are called. Once cryptographic functions are called the module moves into the User State 930. If a request is made to terminate the process, the module will clear all loaded keys from memory before transition to the Un-Initialized State 920. The User State 930 is used to perform all cryptographic functions, not related to key management, that are performed by the cryptographic module 14. As soon as a key-related function is complete, the module transitions back to the Idle State 970. If the cryptographic module 14 is not going to perform key management features it will be loaded with the keys of the current user. At that point, the module enters the Idle State 970 and remains there until either a cryptographic function

is called or the process is ready to end. Keys will be created or modified and stored in the secured SQL database 305. The cryptographic module 14 will clear all key information from memory and transition back to Un-Initialized State 920. If cryptographic functions are requested from the Idle State 970, the module 14 enters the User State 930 to execute the requested cryptographic function. After the requested function is performed, the module re-enters the Idle State 970. In the Idle-State 970 or the Crypto-officer State 940, if the process is ready to end the module clears the keys and returns to the Un-Initialized State 920.

Detailed Description Text (231):
In the Key Entry State 960 the cryptographic module 14 loads the keys obtained from SQL master database 305 for the authenticated user 2. The Initialize function of the Crypto-API library is used by the cryptographic module as a means of initializing the crypto-context with the keys. After successfully loading the keys, the module 14 moves to the Idle State 970.

Detailed Description Text (233):
Three NT accounts will be set up for the server processes to run under. The Transaction Manager and all Non-Cryptographic modules will run under the RSP User account 621. This account will have no access to the file system or the Secure SQL master database 305. The server cryptographic Module 14 will run under one of two accounts. A CRYPTO.sub.13 User account 622 will be used to perform all non-key management cryptographic functions (e.g. encryption, decryption, and indicium generation). This user will have read only access to the Secure SQL master database 305. If key management is required, the cryptographic module will run under a CRYPTO_Officer account 623. This account will be able to create keys and will be able to insert, update, and delete keys from the Secure SQL Database.

Detailed Description Text (238):
Set forth below in Table IV is a table of the various security features used in the functions performed by Transaction Server 180.

Detailed Description Text (240):
An auditing and reporting feature is an amalgam of various other features contained within the system. The server 4 automatically records various data and stores them on the log server 195. Items stored include the User Profile Log and the Indicium Log, which are maintained in databases 196 and 197. In addition, the master server 300 contains individual PSD 20n that contain the Ascending Register 22, the Descending Register 21, and the Refind Register 24. In terms of security functions, server 4 is event dependent. It is event dependent in that the server has event-driven requirements of the user (e.g., when an indicium 24 is created, it is logged).

Detailed Description Text (242):
The User Profile Log contains a record of the information specific to the current user 2n, such as the mailing address, phone number, etc. If any of the parameters within the user profile are modified, then the housekeeping service will in turn up-load the new user profile to the server.

Detailed Description Text (247):
Housekeeping is an independent service which exists on the server 4 and handles all the indicium log updates, user profile updates, rate table updates and new software updates as necessary.

Detailed Description Text (248):
On the client 2 side, after the Transaction Service successfully receives the Handshake Response Object, it sends the following housekeeping request to the server 4: New rate table request and New software request.

Detailed Description Text (258):

The user profile will contain information specific to the current user 2n, such as the mailing address, phone number, and any other information required on PS Form 3601-A and the information returned on PS Form 3601-B. If any of the parameters within the user profile are modified, then the housekeeping service will in turn up-load the new user profile to the server.

Detailed Description Text (260):
On a periodic basis (e.g., 12:00 midnight every day) the server 4 system can run an agent that reviews all log database tables that have changed during the prior 24-hour period. Any changes that have been made are analyzed and matched to the customer record found in the Master Database 305. Purchase, spoilage, and refund information will be marked for a batch transmission to TPS 6.

Detailed Description Text (261):
Data supplied to TPS 6 about such periodic (daily) activity are kept in the Log and Master databases 196, 197 and 305. The two tables used are PSD and Log. All data in these tables are available for review by the USPS as ad-hoc reports.

Detailed Description Text (262):
The records of the various transactions are stored on logs on the server 4. The records of the postage downloads from TPS 6 to are sent to USPS Treasury daily as part of a daily reconciliation. The records of all other financial transactions are sent to TPS 6 (NMATS) each morning. If, for example, $100 in postage were downloaded from TPS 6 USPS to server 4 and server 4 subsequently sold $25 each to users 2i, 2j, and 2k, the logs would indicate the following transactions:

Detailed Description Text (267):
i. Communications and message interfaces with TPS 6 financial institutions

Detailed Description Text (268):
The server 4 notifies the TPS 6 (United States Postal Service financial institution (FDMS)) of all credit card transactions. Credit card and ACH debit card postage download purchases are transacted in real time and stored in log 196, 197 on the server 4. These logs are transmitted to USPS at the appropriate time and in an agreed upon format. The Daily Record of Transactions is forwarded to NMATS every morning and the Daily Account Reconciliation is forwarded to the Treasury each day as well. Postage value downloads purchased by check are recorded by the Transaction Service and forwarded to the Treasury and NMATS as part of the above-mentioned file transmissions.

Detailed Description Text (269):
It should be understood that the present invention is applicable to third party sellers of goods and/or services other than the USPS, where electronic transactions are used by the user/customer to pay for the goods and/or services. Indeed, the present invention is applicable to situations in which the remote service provider 4 also is the third party seller of the goods or services, as contrasted with a brokering or sales agent as in the case of the preferred embodiment described in detail above. Such examples include, without limitations, other package/mail carriers or shipping services, such as Federal Express, UPS, Airborne, Purolator, Roadway, and the like, Postal Services of other countries, tax stamp issuing authorities for state, federal and other governmental agencies, stock certificate issuing entities, and ticket issuing entities (such as tickets for live and movie theatres, sporting events, concerts, travel/transportation such as air, boat, train, bus, subway and the like). In each of these cases, a unique indicium, postal or otherwise, can be generated by the RPS 4, digitally signed by the true customer, downloaded to the customer and printed as a "receipt" locally by the customer who has electronically paid for the purchase via the Internet. The indicium can be scanned at the point of consumption, e.g., when the package enters the mailstream or the shipping company system, or the customer enters the facility where the sporting event or concert occurs. Because each receipt is unique, a duplicate (and

thus a fraudulently obtained copy) can be easily detected and the legitimate version identified, and the offender caught and punished as appropriate. The ease of scanning in and the speed of decoding the two dimensional matrix codes or bar codes incorporated into the indicium, postal or otherwise, renders the process essentially transparent to the customer.

Detailed Description Paragraph Table (1):
TABLE I Transactions Server Actions Transaction Master Server Payment Server Postage Server Customer Server Credit Auth. Transaction Type Server 190 300 190 Log Server 195 450 460 Server 400 Authentication 1. Verify client 1. Provide 1. Log Transactions Provide customer client 2n to server Signature customer information 2. Decrypt public key client request 2. Send 3. Request Transaction customer Summary to lookup Log Server 4. Decipher message 5. Validate customer 6. Send digitally signed and ciphered message Purchase of 1. Verify 1. Increment Manage 1. Log Transactions 1. Decrement 1. Issue Good/services e.g., digital; customer PSD Purchase 2. Send Log to Master check request postage Signature of ascending Process TPS (IBIP descending 2. Receive client register Infrastructure) register response 2. Decrypt 2. Send 2. Request 3. Send response client Transaction postage from to Purchase Request Summary to TPS (USPS) Server 3. Send Log Server 3. Increment purchase Master Request to descending Payment register Server 4. Send 4. Digitally Transaction Sign and Summary to Encrypt Log Server Response 5. Send ciphered message to client Refund 1. Verify client 1. Increment Manage 1. Log Transactions 1. Decrement 1. Issue credit Signature customer PSD Refund 2. Send Log to TPS Provider PSD check request 2. Decrypt ascending Process (IBIP ascending 2. Receive client register Infrastructure) register response Request 2. Send 2. Send 3. Send response 3. Send Transaction Transaction to Purchase Request Summary to Summary to Server to Payment Log Server Log Server Server 4. Digitally sign and Encrypt Response 5. Send digitally signed and ciphered message to client Print 1. Verify client 1. Decrement 1. Create 1. Log Transactions Signature customer PSD Indicia 2. Send Log to 2. Decrypt ascending 2. Create file: IBIP client register of Indicia Infrastructure Request 2. Send 3. Notify 3. Send Transaction Transaction Request to Summary to Server Payment Log Server Server 4. Digitally sign and Encrypt Response 5. Send ciphered message to client Address Change 1. Verify client 1. Log Transactions 1. Update Signature 2. Send Log to Customer 2. Decrypt IBIP Record client Infrastructure 2. Send Request Transaction 3. SendRequest Summary to to Customer Log Server Server Address Cleanse 1. Verify client 1. Log Transactions 1. Cleanse Signature 2. Send Log to TPS Addresses 2. Decrypt (IBIP 2. Create file of client Infrastructure) addresses Request 3. Notify 3. SendRequest Transaction to Customer Server Server 4. Send 4. Digitally Transaction sign and Summary to Encrypt Log Server Response 5. Send ciphered message

Detailed Description Paragraph Table (4):
TABLE IV Security Transaction Security Audit Control Cash Mgt. Compliance Registration SSL3.0 Creation of Customer Record CMLS License Request RC2 Store X.509, Key Pair, License ID MD5 Acquisition SSL3.0 (Download) Purchase RSA Authentication Log Purchase Request Transfer of funds to USPS Daily Log File Upload to CMRS Integrity (Hash) Log Prior/Current Register States banking authority RC2 Encryption Add to individual descending Session Key register Deduct from master descending register Refund RSA Authentication Log Refund Request Add to individual descending Daily Log File Upload to CMRS Integrity (Hash) Log Prior/Current Register States register RC2 Encryption Deduct from master Session Key descending register Printing RSA Authentication Log Indicia(um) Deduct from individual Indicia Log available Integrity (Hash) Log Prior/Current Register States descending register RC2 Encryption Session Key Cleansing RSA Authentication Log Addresses Address Log available Integrity (Hash) RC2 Encryption Session Key Address Change RSA Authentication Log Prior/Current Addresses Daily Log File Upload Integrity (Hash) to MATS/NMATS RC2 Encryption Submit update request to CMLS Session Key Software Change SSL3.0 Store prior software Postage Rate SSL3.0 version off-line Update

Issued US Original Classification (1):
705/35

Current US Original Classification (1):
705/35

Field of Search Class/SubClass (2):
705/35

CLAIMS:

1. A system for conducting Internet based financial transactions comprising:

a client having a processor, a printer, a client authentication module, a module for issuing a transaction request, and a unique digital signature;

a server having a network including a transaction server, a transaction database, a server authentication module, and a receipt generation module; and

an internet connection between the client and the server network;

wherein the transaction execution system further comprises:

an authentication module, wherein the client authentication module and the server authentication modules communicate via the internet connection and are authenticated to each other;

a transaction module wherein, in response to the client and server being authenticated, the client issues a transaction request to the server and the transaction server, in response to a client transaction request, executes an electronic payment transaction at the server and records the transaction in the transaction database, and wherein the server receipt generation module, in response to an executed electronic payment, generates a receipt and transmits said receipt to the client, said receipt comprising the client digital signature and a data set uniquely identifying the executed transaction; and

wherein the receipt is printable by the client printer and the printed receipt is an evidence of payment for the executed transaction.

2. The system of claim 1 wherein the module for issuing a transaction request further comprises means for providing the transaction request with the client digital signature.

4. The system of claim 1 wherein the server further comprises a first server, a firewall and a single TCP/IP port, the first server is connected to the interact connection, the firewall is interposed between the server first server and transaction server so that the transaction server is connected to the network through the single TCP/IP port and the firewall comprises a communication module that operates to limit communications between the internet and the transaction server to client transaction requests identifying the single TCP/IP port.

5. The system of claim 1 further comprising:

a third party seller having a processor and a database; and

a communication channel between the third party seller and the server,

wherein the client further comprises a registration certificate representative of being a consumer registered with said third party seller.

6. The system of claim 5 further comprising a transaction module wherein said third party seller database is updated by said server transaction database.

7. The system of claim 1 further comprising a third party credit facility and a communication link between the third party credit facility and the server, wherein the server further comprises a credit module wherein, in response to a client transaction request, a credit card payment request is made by the server to the third party credit facility, the third party credit facility authorizes the credit card payment and issues an authorization code to the server, and the server transaction database is updated.

8. The system of claim 1 wherein the transaction request further comprises a request to purchase an amount of postage, an addressee data set, and wherein the server transaction database further comprises a pool of postage prepaid by said server, and an account register associated with said client, wherein the client transaction request operates to transfer the requested amount of postage from said pool to said client account register.

10. A method for conducting Internet based financial transactions comprising:

providing a client having a processor, a printer, a client authentication module, a module for issuing a transaction request, and a unique digital signature;

providing a server having a network including a transaction server, a transaction database, a server authentication module, and a receipt generation module;

connecting the client to the server network via an internet connection;

authenticating the client and the server to each other;

issuing a transaction request from the client to the server;

in response to a client transaction request, executing an electronic payment transaction at the transaction server and recording the transaction in the transaction database, generating a receipt at the server receipt generation module, providing said receipt with the client digital signature and a data set uniquely identifying the executed transaction, and transmitting said receipt to the client; and

printing said receipt using the client printer, wherein the printed receipt is an evidence of payment for the executed transaction.

11. The method of claim 10 wherein issuing a transaction request further comprises providing the transaction request with the client digital signature.

13. The method of claim 10 wherein providing the server further comprises providing a single TCP/IP port connecting the first server to the internet connection with said client and limiting communications between the internet and the transaction server to client transaction requests identifying the single TCP/IP port.

15. The method of claim 14 further comprising providing the third party seller with a transaction database and updating said third party seller transaction database by said server.

16. The method of claim 10 further comprising providing a third party credit facility, connecting the third party credit facility and the server via a communication link and in response to a client transaction request, issuing a credit card payment request by the server to the third party credit facility, authorizing the credit card payment by the third party credit facility and issuing an authorization code to the server, and updating the server transaction database.

17. The system of claim 10 wherein issuing the transaction request further comprises issuing a request to purchase an amount of postage, an addressee data set, and wherein the server transaction database further comprises a pool of postage prepaid by said server, and an account register associated with said client, wherein issuing the client transaction request further comprises transferring the requested amount of postage from said pool to said client account register.

Previous Doc Next Doc Go to Doc#

L8: Entry 98 of 124 File: USPT Sep 12, 2000

DOCUMENT-IDENTIFIER: US 6119104 A
TITLE: Composite banking desktop system

Abstract Text (1):
A multi-desktop computer system for a bank or other financial institution includes a plurality of functional desktop routines, each desktop operating on an identical "platform" of object-oriented routines. This "platform" of common object-oriented routines for use by each of the desktops, substantially reduces the design requirements of the desktops in that they only have to be designed to conform to the command structures of the object-oriented routines, and they do not have to be designed to any specific mainframe message structure or protocol. All of the functional desktops may be compiled together, along with the "platform" of object-oriented routines, to form one integral program, where a particular desktop will be activated, depending upon its need. The system enables a user to move between desktops, depending upon the need to activate a particular desktop. The system includes a system database that allows the desktops to share information with one another, such as customer information. The system also includes the capability of locking the user out of particular desktops, if that particular user does not require access to that particular desktop.

Brief Summary Text (3):
Many companies today provide services and keep customer information in mainframe computer systems. In many instances, mainframe computer systems are faster at accessing and processing relatively large amounts of information in comparison to a network of personal computers. However, many mainframe systems have evolved over time to include various capabilities and presently are comprised of various legacy systems, each performing a specific function and having a discrete message structure and protocol for storing and retrieving information. For example, in the area of banking, there may exist a first legacy system for retaining account information, a second legacy system for retaining financial product information, a third legacy system for handling loans, and so on; each system having its own message structure and protocol for accessing and storing information. Such mainframe systems utilized an array of terminals which could be positioned at locations remote from the mainframe.

Brief Summary Text (8):
The present invention provides a multi-desktop computer system for a bank or other financial services institution comprising a plurality of functional desktops, each desktop operating on an identical "platform" of object-oriented routines. The plurality of functional desktops may include a kiosk marketing desktop, a collections desktop, a branch desktop, a call center desktop, a brokerage desktop, and the like.

Brief Summary Text (9):
The present invention is designed to be used with a bank's computer mainframe and an interface server to facilitate communications between the platform of common object-oriented routines and the mainframe. The computer mainframe has a plurality of discrete database and application programs, which preferably include a financial transaction system, a customer information database and a product information database. Each of the object-oriented routines is configured to generate a message

to a discrete database or application program in the mainframe in response to user commands and requests from the functional desktops, and in a protocol appropriate for the particular database or application program.

Brief Summary Text (11):
The plurality of object-oriented routines in the platform preferably includes a configuration object for identifying each of the desktops and for allocating necessary resources to the desktops upon identification, a security object for restricting and controlling access to selected portions of the associated mainframe, a products object for handling requests to a product information database, a customer object for handling requests and commands to a customer information database in the mainframe, and a quotes object for calculating requests for rate quotes.

Brief Summary Text (12):
The marketing kiosk desktop, so named because it is designed to be installed in a stand-alone kiosk at a branch bank or in a shopping mall, includes a graphical user interface which enables a customer to browse through various financial products from the product information database to access and calculate quotes based upon information entered into the marketing platform by the customer using the graphical user interface. Such quotes include retirement quotes based upon the customer's age, retirement age, current salary, annual savings, and rate of return. Other financial products provided by the marketing kiosk may include products related to various borrowing options and checking options that are provided by the bank.

Brief Summary Text (14):
The system facilitates the sharing of information between certain desktops by allowing these desktops to use the same object-oriented routines. For example, it would be advantageous for the teller desktops, the sales desktops, and the collections desktops all to use the customer object, thereby assuring that each desktop has all the customer information available to best serve the customer. Therefore, the system preferably includes an object-database, accessible by the objects, that allows the objects to compile and share information apart from the mainframe database and application programs.

Brief Summary Text (15):
Preferably the system of the present invention also includes a transaction monitor server operatively coupled between the platform and a plurality of mainframes, for logging transactions requested and performed by the platform.

Brief Summary Text (16):
Other object-oriented routines in the platform can include a campaigns object, which allows manipulation of outbound marketing campaigns; a customer object, which provides an interface to customer search and profile retrieval; a credit object, which exposes functionality to new credit product applications and credit checking functionality; a deposit object, which exposes functionality to new deposit product applications; a reports object, for writing report records for retrieval; a preference data object which provides an interface to business data and lists literal strings, and for code/description conversions; a workflow object, which provides business process flow management; a zip code look-up object, which includes zip code look-up functionality; and a promotions object, which supplies promotional information to a user.

Brief Summary Text (17):
Accordingly, it is an object of the present invention to provide a multi-desktop computer system for a bank or other financial services institution which comprises a plurality of functional desktops, a computer mainframe, a plurality of object-oriented routines that are accessible by each of the functional desktops for receiving and processing commands and requests from the functional desktops, and an interface server for providing an interface between the set of object-oriented

routines and the computer mainframe. It is a further object to the present invention that the plurality of functional desktops includes the kiosk-based marketing desktop, a collections desktop, a branch desktop, and a telephone personnel desktop.

Detailed Description Text (2):
As shown in FIG. 1, the composite banking desktop ("CBD") system 10 of the present invention includes a plurality of software routines, referred to as functional desktops 12, each of which operates on a platform 14 of object-oriented software routines. In the preferred embodiment, the plurality of functional desktops 12 and the platform 14 of object-oriented routines are compiled together to form an integral software package operating on a network of computers. The platform 14 includes a messaging transport protocol, such as TCP/IP or ECI, IBM's extended call interface product, generally designated MTP 16, which facilitates the actual communication for the CBD 10 into a mainframe computer 18 of the financial institution. The MTP 16 is preferably interconnected between the CBD 10 and the mainframe 18 by a set of data links 20 such as wide area networks. Additionally, the MTP 16 is linked to a transaction monitor server 21, which is responsible for logging transactions requested and performed by the CBD.

Detailed Description Text (3):
The mainframe computer 18 includes a mainframe interface server 22 for providing a communication interface between the mainframe legacy systems 24 and the MTP 16. The mainframe interface server 22 also provides a communication interface between the financial institution's mainframe 18 and third-party mainframes 26. The financial institution's mainframe includes corporate information repository database ("CIR") 28, which is a consolidated database of customer addresses, account data, relationship data, and the like; an on-line delivery system ("OLDS") 30 which is a primary database for storing information on all customer accounts; a credit system ("ASAP") 31; a product information repository ("PIR") 32, which is a data base containing information on the bank's products; a host maintenance link interface to an ATM network ("HML") 34 and a HOGAN 36 transaction posting system. The OLDS 30 provides automated teller and branch balancing and control functions such as deposit account transactions, credit account transactions, bill payment transactions, teller transactions, and the like. As mentioned above, the HML 34, OLDS 30, CIR 28, PIR 32, and HOGAN 36 mainframe systems are known collectively as legacy systems.

Detailed Description Text (5):
The plurality of the functional desktops 12 include a marketing kiosk desktop 36, a collections desktop 38, a plurality of branch desktops 40, a plurality of call center desktops 42, and a plurality of brokerage desktops 44. The collections desktop 38, the branch desktops 40, the call center desktops 42 and the brokerage desktops 44 are for use by agents of the financial institution when dealing with a customer or potential customer of the financial institution. Such interface between the agent and the customer, as will be appreciated by those skilled in the art, include face-to-face meetings, telephone conferences, computer communication over the modem, written correspondence and the like.

Detailed Description Text (7):
The platform of object-oriented routines 14 is essentially a plurality of reusable, object-oriented routines, each of which is accessible by substantially all of the desktops. Each object-oriented routine is written in an object-oriented software architecture, such as Microsoft.RTM. OLE Standard Architecture. Essentially, each object-oriented routine 14 is configured to process a message or command from a desktop routine and format the message for the mainframe 18. The mainframe interface server 22, upon receiving the re-formatted message, compares the re-formatted message with a transaction table to determine which of the legacy systems 24 is to be linked with the re-formatted message.

Detailed Description Text (8):
The plurality of object-oriented routines 14 preferably includes a customer object 64, which provides an interface to customer search and profile retrieval; a credit object 66, which exposes functionality to new credit product applications and credit checking; a deposit object 68 which exposes functionality to new deposit product applications; a reports object 70, which facilitates the writing of report records for retrieval via a commercially available database system report writer; a user object 72, which contains authentication and access control functionality for the users of the CBD desktops 12; a referral object 74, which allows referrals to other departments within the bank; a presentations object 76, which handles sales presentations via audio, video, slide show, and the like; a logging object 78, which provides system-wide logging facilities; a printing object 80, which provides standard printing interfaces to commercially available publishing tools and also provides for document merging, queuing and printing; a workflow object 82, which provides business process flow management; a configuration object 84, which allows definitions of workstations/desktops as CBD desktops and allocates resources to the particular workstations running the CBD desktop thereon; a reference data object 86, which provides an interface to business data and lists, literal strings, and code/description conversions; a quotes object 88, which provides a quotes and calculation engine; a cross-sell object 90, which, given available customer data, will suggest to a sales representative possible cross-sell products; an error object 92, which provides system-wide errors stacked in display functions; a products object 94, which facilitates access to the PIR database 32 in the mainframe 18 and returns product rates and fee information upon request; a campaigns object 96, which allows manipulation of outbound campaigns; a branch object 98, which allows branch search and details look-up; a zip code look-up object 100, which provides zip code look-up functionality; a telephony object 102, which provides an interface to telephone disposition systems and inter-site voice/data transfer; and a scripting object 104, which provides the ability to control a user's navigation in a particular desktop using a prerecorded script. Several of the above objects 14 access and write to a CBD database 106. As will be described in further detail below, the CBD database allows the objects 14 to store and share information without necessitating access to any legacy systems.

Detailed Description Text (10):
At a central location, a data center 212 comprises a plurality of servers interconnected on an FDDI LAN structure 214, which enables communication to and from the mainframe 18. Each location can be connected to the data center 212 by a pair of hubs 216, by direct coupling 218 to the FDDI LAN structure, or through a frame relay communications system 220 provided that can be provided by an independent third party provider. Although not indicated in FIG. 2, the marketing kiosk 200 may be connected to the data center 212 by any of these connections. A legacy gateway server 234 provides access to the mainframe legacy systems from the FDDI ring and the ECI server 236 maintains the MTP object 16 as described above. The plurality of servers may further include a database server 222 which may support the CBD database 106 (see FIG. 1), and a gateway server 224 may be provided to facilitate the transfer of data between the mainframe 18 and the database server 222. An IP addressing server 226, a systems management/maintenance server 228, a machine name to IP translation server 230, IP logon control server 232, and a credit application/processing server (not shown) may also be provided in the data center 212.

Detailed Description Text (15):
As shown in FIG. 6, the collections desktop 38 includes a graphical user interface to facilitate use of the desktop by a collections agent. Primarily, to provide an effective and valuable service to the customer, the collections agent needs to be able to review the overall relationship of the customer with the particular financial institution, access and manipulate account delinquency details, access the most recent contacts between the customer and the financial institution, and review associated customer correspondence and credit bureau reports. Accordingly,

the collections desktop 38 is divided into two areas or folders: the customer folder 140 and the collections folder 142. The customer folder 140 provides customer information to the agent such as the different financial products presently used by the customer is presently taking advantage of (see the Accounts area 144), demographic details 146, miscellaneous information about the customer 148 (entered, for example, by other employees of the financial institution using other desktops), history of past contacts with the customer 150 (to avoid, for example, unnecessary or redundant contacts with the customer), and the like.

Detailed Description Text (16):
The customer folder 140 is preferably used in a similar manner by each desktop that provides a graphical user interface for an employee of the financial institution who deals directly with the customer. For example, the customer folder 140 is preferably used by the sales desktop 46, the teller desktop 48, the fulfillment desktop 52, the telesales desktop 54, the teleservice desktop 56, and the trading desktop 60. The customer object 64 is preferably accessed by these desktops to generate and maintain the customer folder 140 therewithin. Upon selection of a particular customer within a desktop, the customer object 64, in response to an update request, will access the CBD database 106 to update the customer folder 140 within that desktop. The customer object 64 may also access the customer information from the CIR database 28. The desktop has the ability to modify or add to the customer information in the customer folder 140, which will update the customer information appropriately in the CBD database 106 and/or CIR database.

Detailed Description Text (19):
As shown in FIG. 7, the sales desktop 46 (or the telesales desktop 54) includes a graphical user interface to facilitate the use of that desktop by a sales consultant, agent or salesperson within the bank. Such a desktop is available both to the telesales locations 202 and the branch locations 204. The sales desktop 46 includes a products and services table 152 that displays all products and services offered by the financial institution. By activating an item in the products and services table 152, the sales consultant is able to access more information on a particular product or service and is able to indicate in a database that the particular client is interested in the product activated. Such information preferably is accessed from the CBD database 106 or the PIR legacy system 32 using the products object 94 (see FIG. 1). Also included on the sales desktop 46 is an open/in process table "shopping cart" 154 that lists for a sales consultant all of the products in which that a particular customer already has participated or shown an interest.

Detailed Description Text (22):
The Big Five Focus sub-folder guides a customer or sales consultant through a series of questions which focus on one of five areas: education planning, retirement planning, debt payment, borrowing, and accumulation of wealth. Based upon how a customer answers the questions, the desktop recommends products best suited to the customer's needs. The Products folder will allow a customer or sales consultant to access details about the products available such as options, rates and fees, and the like. The Products sub-folder will also allow the customer to fill out a generic application which can be used to apply for any or all of the products available. This generic application will pull information from the customer folder, preferably from the CBD database 106, to fill in the information already available for the customer. The generic application screen will utilize the credit object 66, the deposit object 68 and the customer object 64 (shown in FIG. 1) Therefore, by sharing information between desktops, the application process is shorter and easier. Finally, the What-Ifs sub-folder provides the agent/customer with quoting or calculating screens, referred to as "what-if" screens, which include screens for retirement planning, education planning, savings planning, mortgage planning, and the like. These screens will be similar to, or the same as, the "what-if" screens used in the marketing kiosk desktop 36 described above.

Detailed Description Text (26):
The primary role of the products object 94 within the CBD system 10 is to supply products, rates and fees information to the desktops 12 upon request. The rates and fees information is obtained from the PIR database 32 within the mainframe (see FIG. 1). These data are accessed from the PIR 32 and downloaded into the CBD database 106. The download of the data from the PIR database 32 to the CBD database 106 is a function of a separate program operating within the CBD, whose primary purpose is for such a download. The products object 94 will always assume that the data within the CBD database 106 is up-to-date and accurate. Thus, the products object 94 will not necessarily directly request refreshes of the CBD database.

Detailed Description Text (27):
FIG. 8 illustrates the high level class hierarchy within the product object 94. Upon startup, the product object 94 will create a complete set of productxxxx objects 110 internally. The productxxxx objects 110 are illustrated as "productxxxx," where "xxxx" contains the product identification. The product factory object 112, created upon start up of the products object 94, contains a product configuration object 114 and a result storer 116. The complete set of rates and fees are stored in the result storer 116, which keeps track of when it was last updated. The result storer 116 updates itself after a predetermined amount of time. The result storer 116 accesses the CBD database 106 through a data access layer 118. As described above, the configuration object 84 follows the definition of a work station operating a desktop as an entity within the CBD system.

Detailed Description Text (32):
The workflow object 82 facilitates the mapping of business processes performed into discrete tasks which are governed by a predefined set of rules. Tasks of work may be grouped into processes and, in turn, processes are grouped to build a hierarchy of workflow automation.

Detailed Description Text (34):
The quotes object 88 is responsible for undertaking financial calculations on behalf of a desktop. It can handle both credit and deposit type calculations and is completely independent of the products object 94. As shown in FIG. 10, the class hierarchy for the quotes object 88 includes a quote rate table object 134, a deposit quote object 136 and an installment loan quote object 138, all of which are created upon demand.

Detailed Description Text (36):
The referral object 74 is accessible by a desktop and will allow the user to input referrals, input the status of referrals and update a referral status. A referral occurs when a bank employee refers a non-customer (or existing customer) to a salesperson in a specialty line of business for follow-up on potential sale of a product. In the event of a sale, the referring employee gets compensated commensurate with the type of product sold. The referral object 74 provides an electronics referral a necessary database for tracking the life cycle of a referral.

Detailed Description Text (37):
In summary, the present invention provides a multi-desktop computer system for a bank or other financial institution comprising a plurality of functional desktops, each desktop operating on an identical platform of reusable, object-oriented routines. This platform of common object-oriented routines for use by each of the desktops substantially reduces the design requirements of the desktops in that they need only conform to the command structures of the object-oriented routines, and not to any specific mainframe message structure or protocol. All of the functional desktops may be compiled together, along with the platform of object-oriented routines, to form one integral program, where a particular desktop will be activated, depending upon its need. Furthermore, the CBD system enables a user to move between desktops, depending upon the need to activate a particular desktop;

and the CBD system includes an internal database that allows the desktops to share and update information with one another. The system will also have the capability of locking a user out of particular desktops, if that particular user does not require access to that particular desktop.

Issued US Original Classification (1):
705/35

Current US Original Classification (1):
705/35

Field of Search Class/SubClass (1):
705/35

US Reference US Original Classification (14):
705/35

US Reference US Original Classification (18):
705/35

US Reference US Original Classification (21):
705/35

US Reference US Original Classification (23):
705/35

US Reference US Original Classification (24):
705/35

US Reference US Original Classification (25):
705/35

US Reference US Original Classification (27):
705/35

US Reference Group (14):
5710889 19980100 Clark et al. 705/35

US Reference Group (18):
5864843 19990100 Carino, Jr. et al. 705/35

US Reference Group (21):
5913202 19990600 Motoyama 705/35

US Reference Group (23):
5930764 19990700 Melchione et al. 705/35

US Reference Group (24):
5933816 19990800 Zeanah et al. 705/35

US Reference Group (25):
5940811 19990800 Norris 705/35

US Reference Group (27):
6023684 20000200 Pearson 705/35

Other Reference Publication (1):
Premeriani et al, "An Object-Oriented Relational Database", Communications of the ACM, vol. 33, No. 11, pp. 99, Nov. 1990.

Other Reference Publication (2):
"Digital Equipment's New Software Framework", Financial Express, p. 5, Dialog File 16:PROMT, Feb. 22, 1994.

CLAIMS:

1. A multi-desktop computer system for a financial institution, comprising:

a plurality of functional desktops, including a branch desktop and a financial service agent desktop;

a computer mainframe having a plurality of discrete databases and application programs, including a financial transaction system, a customer information database, and a product information database;

a plurality of object-oriented routines, each of said routines being accessible by the functional desktops, for receiving and processing commands and requests from the functional desktops;

an interface server for providing an interface between the object-oriented routines and the discrete database and application programs; and

a system database, accessible and modifiable by the functional desktops through at least one of the object-oriented routines, whereby the system database allows the functional desktops to share information with one another;

wherein the object-oriented routine is configured to generate a data request message to a particular discrete database or application program in response to a data update command or request from a functional desktop, and the object oriented routine is further configured to update the system database with data received from the particular discrete database or application program in response to the data update command.

2. The multi-desktop computer system of claim 1, wherein each of the object-oriented routines is configured to generate a message to a selected one of said databases or application programs, in response to the commands and requests from the functional desktops, in a message structure specific to said selected one of said databases or application programs.

3. The multi-desktop computer system of claim 2, wherein each of the discrete databases and application programs has its own specific protocol requirements, and the system further comprises a communication object-oriented routine adapted to satisfy the protocol requirements.

5. The multi-desktop computer system of claim 4, wherein the plurality of object-oriented routines include:

a products object for handling requests to the product information database;

a customer object for handling requests and commands to the customer information database; and

a quotes object for handling and calculating requests for rate quotes.

6. The multi-desktop computer system of claim 1, wherein the object-oriented routine is a customer object and the discrete database or application program is a customer information repository legacy system.

7. The multi-desktop computer system of claim 6, wherein several of the desktops are configured to display a customer folder that presents customer information

stored in the system database.

9. The multi-desktop computer system of claim 1, wherein the object-oriented routine is a products object and the discrete database or application program is a products information repository legacy system.

10. A multi-desktop computer system for a financial institution, comprising:

a plurality of functional desktops, including a branch desktop and a financial service agent desktop;

a computer mainframe having a plurality of discrete databases and application programs, including a financial transaction system, a customer information database, and a product information database;

a plurality of object-oriented routines, each of said routines being accessible by the functional desktops, for receiving and processing commands and requests from the functional desktops;

an interface server for providing an interface between the object-oriented routines and the discrete database and application programs;

a plurality of mainframe systems and the interface server provides an interface between the platform and each of the mainframe systems; and

a transaction monitor server, operatively coupled between the object oriented routines and the plurality of mainframe systems, for logging the transactions requested and performed by the discrete database and application programs.

Previous Doc Next Doc Go to Doc#